DEPARTMENT OF THE NAVY
NAVAL SUPPLY SYSTEMS COMMAND
5450 CARLISEE PIKE
PO BOX 2050
MECHANICSBURG PA 17055-0791

TELEPHONE NUMBER
COMMERCIAL
AUTOVON
IN REPLY REFER TO:
5239
63D
SEP 0 4 2001

From: Commander, Naval Supply Systems Command

Subj: NAVSUP DEPLOYMENT OF DOD/NAVY PUBLIC KEY INFRASTRUCTURE (PKI)

Ref: (a) ASD Memo of 12 Aug 00
(b) ASD Memo of 17 May 01 (NOTAL)
(c) PKI Plan for the DON of 29 Nov 00 (NOTAL)
(d) NAVSUP ltr 5239 63D of 25 Aug 99

Encl: (1) Definition of Terms
(2) PKEI Roles and Responsibilities
(3) Application PKEI Process
(4) NAVSUP PKEI with iPlant Web Server
(5) NMCI and PKEI Interoperability

1. This policy letter reiterates established DoD requirements and milestones contained in references (a) and (b), and outlines NAVSUP's Public Key-Enabling Infrastructure (PKEI) technical architecture determined essential for a successful Claimancy implementation. Specifically,

a. Addressees will comply with the following DOD PKI requirements and milestones:

(1) Server Certificate Requirement. All unclassified private web servers ("non public" web servers containing information not intended for the public) shall be using Class 3 DoD PKI server certificates for server authentication via Secure Socket Layer as a minimum by December 2000.

(2) Network Requirement. All DoD unclassified networks shall be enabled for hardware token, certificate-based access control no later than October 2002 (using the Class 3 Common Access Card (CAC)). Unclassified networks supporting Mission Category I systems will subsequently migrate to Class 4 certificates by December 2003.

(3) User Requirement. All DoD users shall be issued Class 3 DoD PKI certificates by October 2002 and shall use certificates for client authentication to PKEI web applications and for signing all email and encrypting email as appropriate.

(4) Email and Application Requirement. Email in all environments and all web-enabled Mission Category I, II, and III systems, as defined in enclosure (1) and "non public", operating on unclassified networks shall employ public key technology via Class 3 certificates at a minimum. These systems shall require client authentication using Class 3 user certificates by this same date of October 2002.

(5) Application Requirement. All Mission Category I systems operating on unencrypted networks shall migrate to the Class 4 certificate and require client authentication via Class 4 user certificates, i.e., CAC, not later than December 2003.

(6) Application Requirement. Not later than September 30, 2007, all remaining applications operating in all environments shall use Class 4 DoD PKI.

b. Reference (c) is the PKI Implementation Plan for the DON and provides amplifying guidance for the above requirements.

c. Local Navy application-owner Program Managers are responsible for implementing the aspects of PKI within their applications. The migration of NAVSUP applications using our Navy Acquisition (NA) pilot PKI certificates shall be transitional in nature, i.e., applications shall continue to accept NA certificates until they expire and also accept DoD certificates. This will ensure that all users will have adequate time and opportunity to be issued DoD certificates.

d. Enclosures (2) - (5) provide PKEI roles and responsibilities, highlight the process, and diagram the architecture and NMCI and PKEI Interoperability.

2. This letter supercedes reference (d).

3. Our administrative point of contact is Charlene F. Tallman, SUP 63D at 717-605-1432 (DSN 430) and technical point of contact is Richard Luckenbill, SUP 06D at 717-605-7676 (DSN 430).

CAPT R.N. RHEA
By direction

DISTRIBUTION (see page 3)

Subj: NAVSUP DEPLOYMENT OF DOD/NAVY PUBLIC KEY INFRASTRUCTURE (PKI)

DISTRIBUTION:
FISC Jacksonville (Code CO)
FISC Norfolk (Code 00)
FISC Pearl Harbor (Code 00)
FISC Puget Sound (Code 00)
FISC San Diego (Code 00)
FISC Yokosuka (Code 00)
FMSO (Code 9)
FOSSAC (Code 00)
NALC Mechanicsburg (00)
NAVICP (Code 00)
NAVPETOFF (Code 00)
NAVTRANS (Code 00)
NEXCOM (Code 00)

Copy to:
FISC Jacksonville (Code 66)
FISC Norfolk (Codes 12, 80.1)
FISC Pearl Harbor (Codes 95S/D)
FISC Puget Sound (Code 44.1)
FISC San Diego (Code 31)
FISC Yokosuka (Code 30IS)
FMSO (Codes 94, 941, 941-INFOSEC Team, 94E, 95B, 961)
FOSSAC (Code 06)
NALC Mechanicsburg (Code 20)
NAVICP (Codes 041, 04E, 0416, 054, 0542, 05422.03, 0543, 05733, M043, M0433.01, P045.25, P089, P0892, M0426, P042)
NAVPETOFF (Code 10)
NAVSUP (X32 and Codes 02XB, 33C)
NAVTRANS (Code 06)
NEXCOM (Code IA)

Definition of Terms

Assurance Level - The level of assurance of a public key certificate is the degree of confidence in the binding of the identity to the public keys and privileges. Personnel, physical, procedural and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. This document references enabling requirements for the following 2 classes:

Class 3 - intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that require identification of an entity as a legal person, rather than merely a member of an organization. This assurance level requires that the end user register in person. This assurance level has been subdivided into components distinguished by protection of the private key either in software or hardware tokens. Software storage of the private key is acceptable in some environments, but per Ref (a), DoD will be migrating near-term to protection of the private key on hardware tokens, particularly the Common Access Card. Hence, Class 3-enabled applications must include an interface to a hardware token supported by the DoD PKI. This hardware token based assurance level, designated "Class 3 Hardware" offers a higher degree of assurance and technical non-repudiation than software based Class 3.

Class 4 - intended for applications handling medium to high value information in any environment. These applications require identification of an entity as a legal person, rather than merely a member of an organization. This level requires a hardware token for protection of private key material. The combination of all security controls that contribute to this assurance level involves a higher level of robustness than that required for Class 3. Not all environments require Class 4 operation near-term, but in accordance with Ref (a), DoD will gradually migrate to Class 4 usage across the Department, so applications should ensure Class 4 interoperability when feasible to allow for migration strategies that are as transparent as possible for its user community.

Mission Category - Applicable to information systems, the mission category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters combat mission. Mission categories are primarily used to determine requirements for availability and integrity services. DoD will have three mission categories:

Mission Category I - Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. Information in these systems must be absolutely accurate and available on demand (may be classified information, as well as sensitive and unclassified information).

Mission Category II - Systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness (may be classified information, but is more likely to be sensitive or unclassified information).

Mission Category III - Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short term (may be classified information, but is much more likely to be sensitive or unclassified information).

Network - A network is composed of a communications medium and all components attached to that medium, including two or more computers, whose responsibility is the electronic exchange of information using a cohesive set of protocols.

Private Web Server - A web server that is designed for and/or provides information resources that are limited to a particular audience (i.e., DoD) or a subset thereof. (This includes web servers that provide interfaces to e-mail systems.) Any DoD operated web server that provides any information resources that are not intended for the general public shall be considered a private web server and is subject to this policy. A private web server restricts or attempts to restrict general public access to it. The common means of restriction are by the use of domain restriction (e.g., .mil and/or .gov), filtering of specific Internet Protocol (IP) addresses, User ID and/or password authentication, encryption (i.e., DoD certificates), and physical isolation. Personal web servers (i.e., those that only allow one user and are only accessible from the machine to which it is installed) are not subject to this memorandum.

Public Key-Enabled Application/Web Server/Network - A Public Key-Enabled (PK-Enabled) application or web server or network is one that can accept and process a DoD PKI X.509 digital certificate to support one or more application, server, or network-specific functions (digital signature, data encryption support, system/network access) that provide security services. PK-enabled applications interoperate with the DoD PKI to access public key certificates, revocation information (e.g. Certificate Revocation List (CRL)), and general information in public directories or repositories.

Public Key Infrastructure - The framework and services that provide the generation, production, distribution, control, tracking and destruction of public key certificates.

Token - A device (e.g., floppy disk, Common Access Card, smart card, PC Card, Universal Serial Bus device, etc.) that is used to protect and transport the private keys of a user. Per Ref (a), the primary hardware token selected for DoD use is the Common Access Card.

Web Application - Web browser and other distributed applications characterized by a web interface and both back-end (server) and front-end (client) software.

PKEI Roles and Responsibilities

DoD/DON/NAVSUP: Provide the Infrastructure

Program Managers:

- Certify and Accredit the Systems/Applications
- PKEI the Applications
- Educate Users
- Update/Develop any needed Service Level Agreements
- Fund Application-Unique Requirements

Individual Users:

- Provide accurate required personal information to the Navy Registration Authority, Local Registration Authority (LRA), or Trusted Agent (TA)
- Obtain identity certificate
- Obtain electronic mail (e-mail) signature certificate and e-mail encryption certificate
- Safeguard private keys
- Report any suspected compromise of private keys
- Create and store backup copy of certificates
- Trust the applicable Root CAs by loading them and/or properly configuring their browser
- Abide by procedures governing the PKI system regarding the use of certificates and using them only for their intended purpose only

Enclosure (2)

Application PKEI Process

- Ensure application is DITSCAP accredited or operating under an IATO.

- Install a DoD PKI server certificate on the web server (and all associated web servers) and use the cert for server authentication via SSL.

- Alert users early of the PKE process - the more they hear about what is going on... the easier it will be.

- Transition users over time (today - access with userid/password, tomorrow - userid/password and PKI cert and by Oct 2002, and earlier if possible, access application via DoD PKI cert only).

- Add browser check (NAVSUP requirement) to the homepage (for first time users to insure they are using a browser with 128-bit strong encryption - meeting our standard). (Infosec will provide the code.)

- Link the homepage to the NAVSUP user registration page to load DoD cert data and email address to the Master LDAP directory.

- Configure the application web server to communicate with the Validator (EVA) for determining certificate validity.

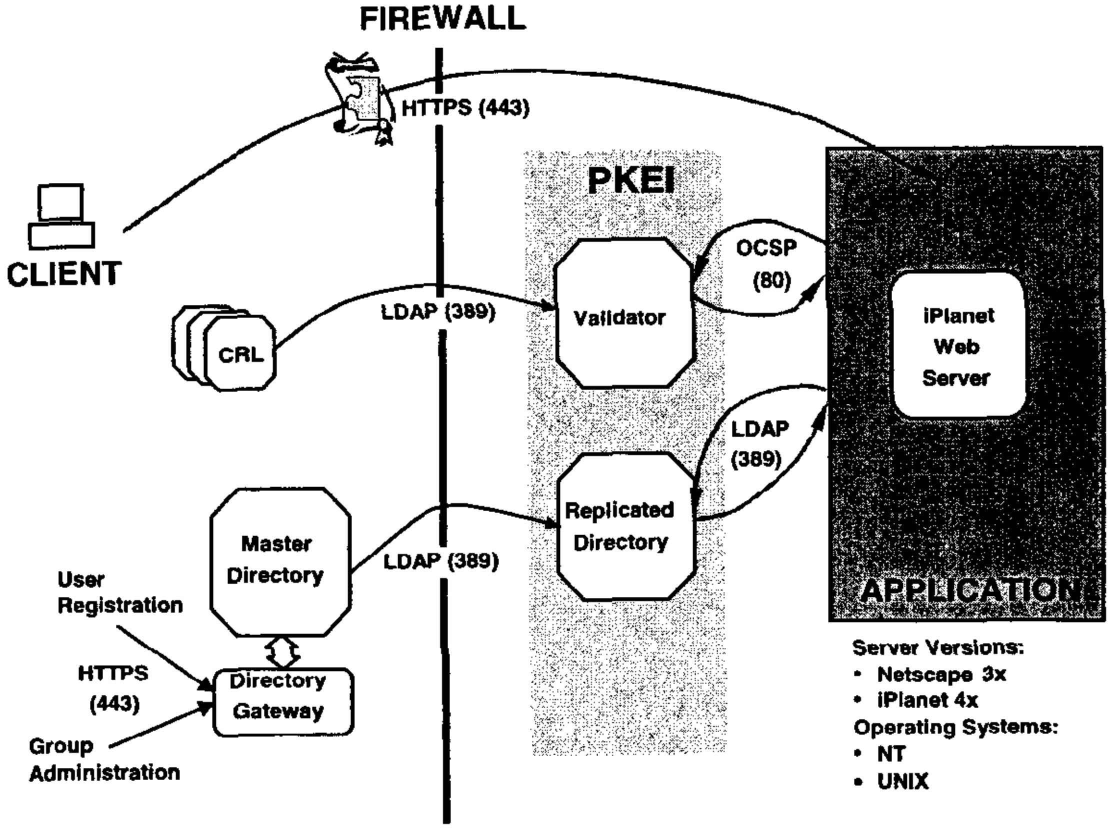
- Establish a local (secondary LDAP directory) directory for access control and configure the application web server to communicate with the directory.

- Establish Master LDAP account with ORC for management access to the Master directory for assigning individual access rights and for receiving directory replications from the Master directory. (See Directory Management at www.pki.navy.mil).

Test application to ensure that DoD PKI certs work with both Netscape and MSIE 5.5 browsers.

Enclosure (3)

NAVSUP PKEI with iPlanet Web Server

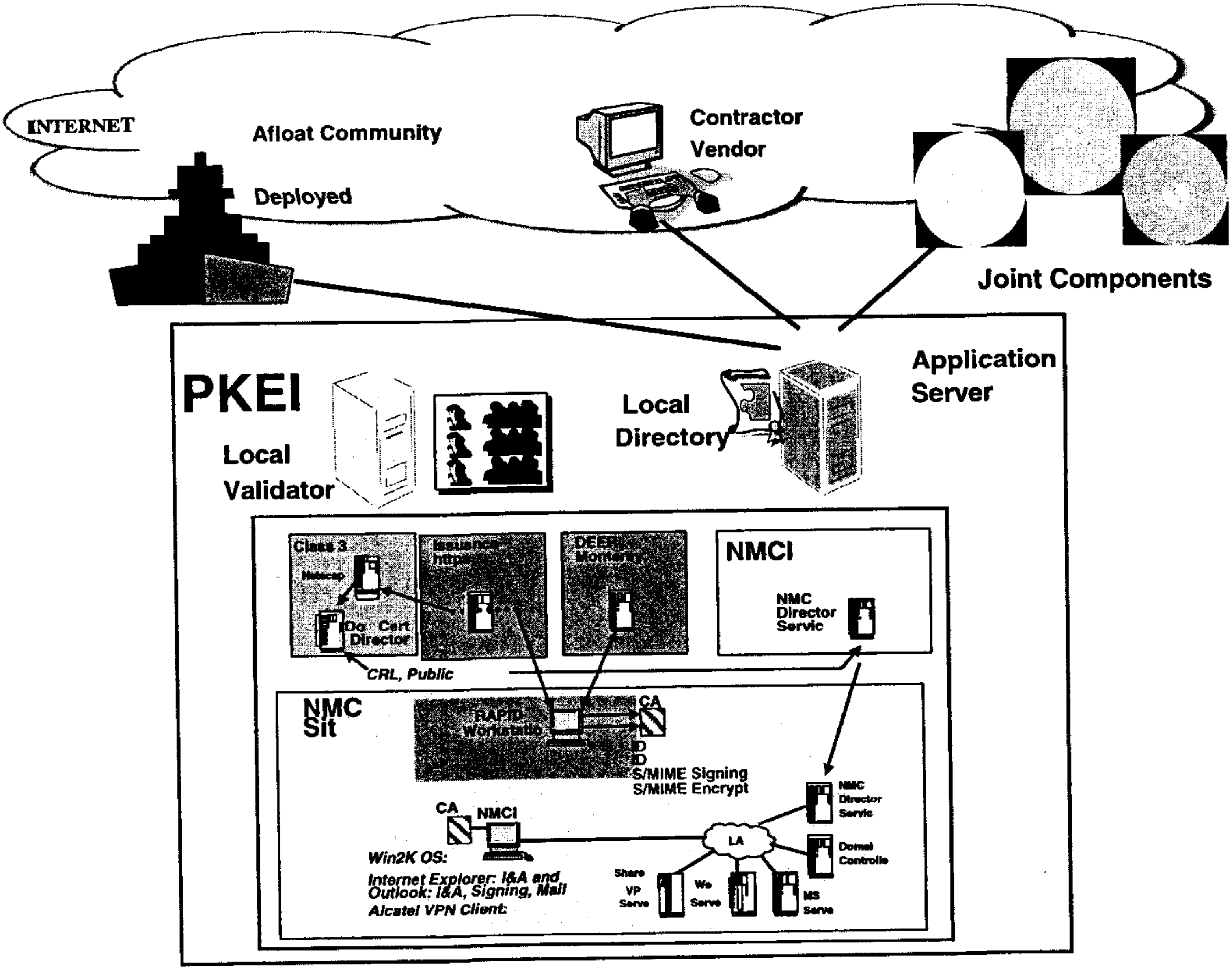


Server Versions:
- Netscape 3x
- iPlanet 4x

Operating Systems:
- NT
- UNIX

ENCLOSURE(4)

NMCI and PKEI Interoperability



ENCLOSURE(5)